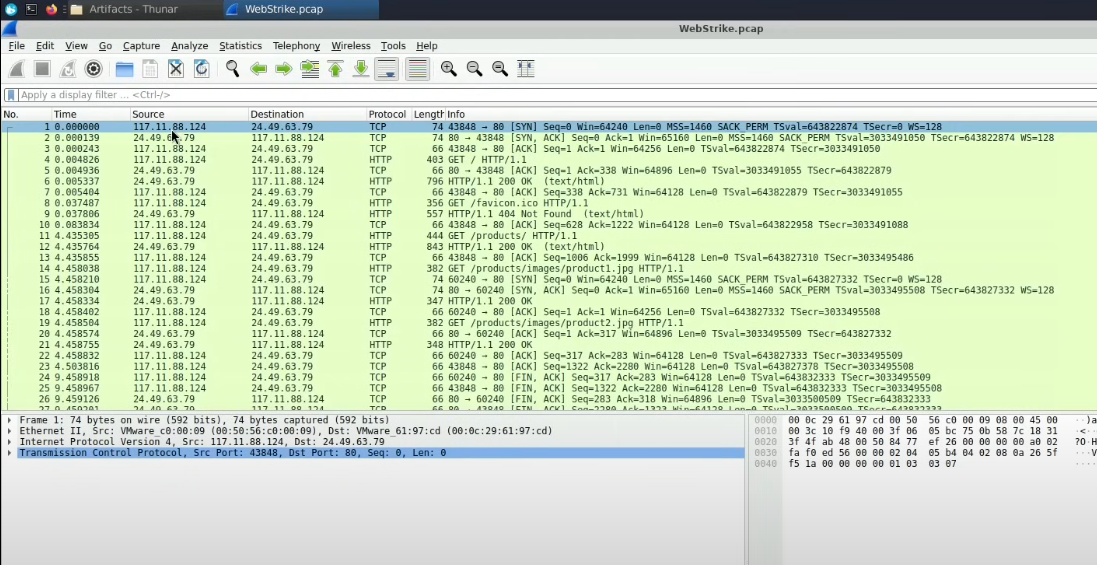
### ****Web Strike Lab****

**Objective:**  
A suspicious file was identified on the company's web server, triggering alerts within the internal network.  
To investigate the issue, the network team captured the related network traffic and generated a PCAP file.  
Analyze this PCAP file to determine how the file reached the server and whether any unauthorized activity occurred.

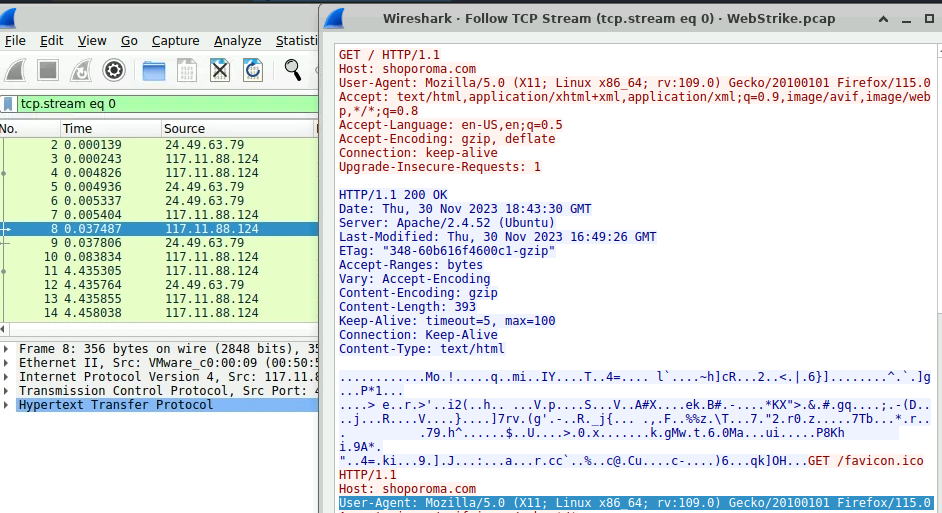
**This exercise is based on a hands-on lab from \*\*Ciberdefense\*\*, a training platform focused on cybersecurity practices and threat analysis.**



1. **Identifying the geographical origin of the attack facilitates the implementation of geo-blocking measures and the analysis of threat intelligence. From which city did the attack originate?**

abuseip : 117.11.88.124, Location Tianjin

1. **Knowing the attacker's User-Agent assists in creating robust filtering rules. What's the attacker's Full User-Agent?**

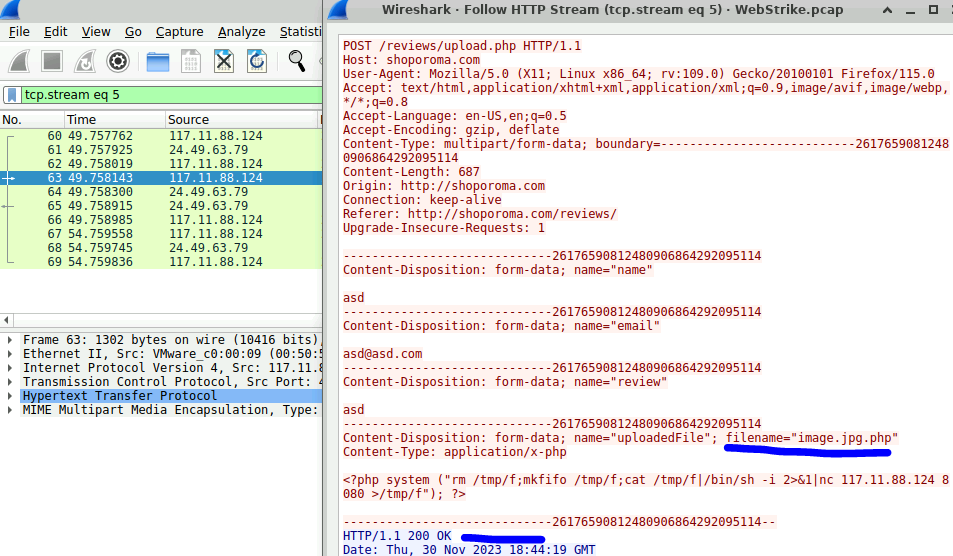


Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

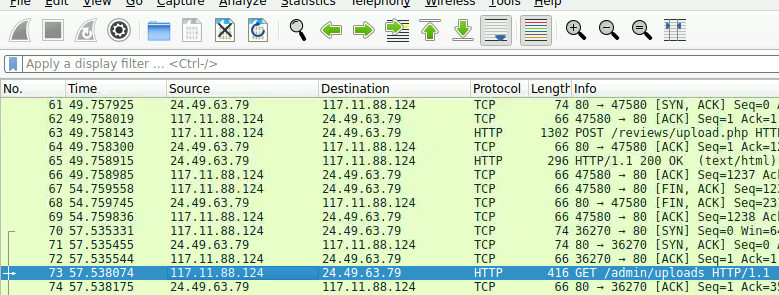
1. **We need to determine if any vulnerabilities were exploited. What is the name of the malicious web shell that was successfully uploaded?**

I filtered the methods that use POST, since uploading a file to a server is typically done via POST requests.

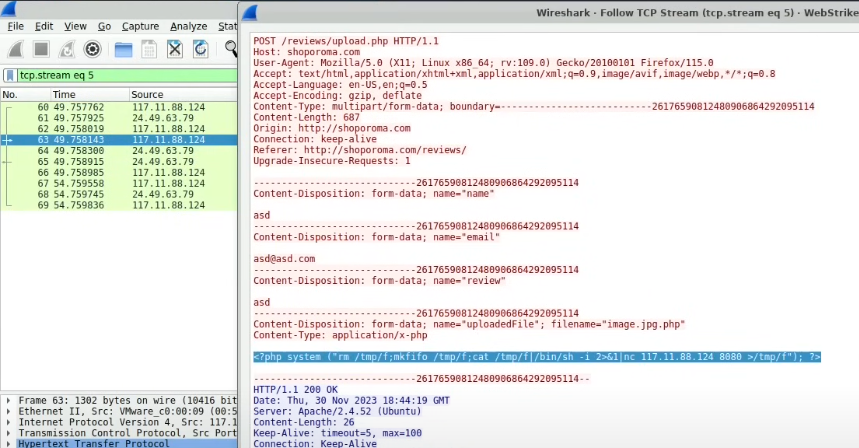
Example filter: ip.src == 117.11.88.124 and http.request.method == "POST"



1. **Identifying the directory where uploaded files are stored is crucial for locating the vulnerable page and removing any malicious files. Which directory is used by the website to store the uploaded files?**



1. **Which port, opened on the attacker's machine, was targeted by the malicious web shell for establishing unauthorized outbound communication?**



8080

1. **Recognizing the significance of compromised data helps prioritize incident response actions. Which file was the attacker attempting to exfiltrate?**

I filtered by the port and the attacker's IP address to view the network traffic sent from port 8080 to the attacker. This traffic represents the files the attacker was accessing.

Filter used: (tcp.port == 8080) && ip.dst == 117.11.88.124

The Linux passwd file contains information about all the users on the system.  
We can see the contents of the passwd file, and the attacker used curl to download it.



